O‘ZBEK TILIDAGI KONFIDENSIAL MATNLARNI ANIQLASH UCHUN TRANSFORMER MODELLAR VA GIBRID TASNIFLASH MEXANIZMLARIGA ASOSLANGAN DLP TIZIMI

Bozorov Obidjon Norqobilovich

katta o’qituvchi, Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti, Tashkent, O‘zbekiston
E-mail: o.bozorov@nuu.uz

KEYWORDS

konfidensial axborot, DLP tizimi, matn tasniflash, mashinali o‘qitish, DistilBERT, ML.NET, ONNX, NER

ABSTRACT

Ushbu maqolada konfidensial axborotlarning ruxsatsiz chiqib ketishini (data leakage) aniqlash uchun mashinali o‘qitishga asoslangan matn tasniflash moduli va uning asosida yaratilgan “KARCHKOOT” DLP (Data Loss Prevention) tizimi taqdim etilgan. Maqolaning ilmiy yangiligi o‘zbek tili uchun qoida, NER va transformer modelini birlashtiruvchi gibrid tasniflash arxitekturasi hamda soxta salbiy holatlarni kamaytirishga qaratilgan ko‘p bosqichli qaror qabul qilish mexanizmini ishlab chiqishdan iborat. Tasniflash moduli ko‘p tilli DistilBERT modelini o‘zbek tilidagi konfidensial hujjatlar korpusida fine-tuning qilish va ONNX orqali C#/.NET muhitiga integratsiya qilish yo‘li bilan qurilgan. Miqdoriy baholash binar (konfidensial / ochiq) tasniflash masalasi sifatida 1 321 ta test faylida o‘tkazilgan; tizim 94,7% Accuracy, 91,5% Precision, 94,8% Recall va 93,1% F1-mezon ko‘rsatkichlariga erishdi. Ablation tahlili, baseline modellar bilan qiyoslash, obfuskatsiyaga chidamlilik va tahdid modeli tahlili keltirilgan. Tizim bir qator davlat tashkilotlarida amaliyotga tatbiq etilgan.

KIRISH

Raqamli transformatsiya sharoitida tashkilotlar faoliyatining markazida turuvchi axborot resurslari hajmi tobora ortib bormoqda. Shu bilan birga konfidensial axborotlarning ruxsatsiz chiqib ketishi (data leakage) axborot xavfsizligining eng dolzarb muammolaridan biriga aylandi. Bunday hodisalar moliyaviy zarar, obro‘ga putur yetkazish va huquqiy oqibatlar bilan bog‘liqdir. Tahlillar shuni ko‘rsatadiki, sizib chiqishning katta qismi tashkilot ichidagi foydalanuvchilar (insayderlar) va tashqi axborot tashuvchi qurilmalar orqali yuzaga keladi.

Konfidensial axborotlarni himoyalashda DLP (Data Loss Prevention) tizimlari keng qo‘llaniladi: ular ma’lumotni harakatda (data-in-motion), foydalanishda (data-in-use) va saqlashda (data-at-rest) nazorat qiladi. Biroq mavjud xorijiy DLP yechimlarining aksariyati asosan kalit so‘zlar va regulyar ifodalarga tayangan an’anaviy aniqlash usullaridan foydalanadi, bu esa kontekstga boy hujjatlarda yuqori soxta salbiy (FN) va soxta ijobiy (FP) ko‘rsatkichlariga olib keladi. Bundan tashqari, ushbu tizimlar o‘zbek tilining morfologik va yozuv xususiyatlarini (aglutinativ tuzilma, lotin/kirill alifbolari, ko‘chma so‘zlar) yetarlicha hisobga olmaydi.

So‘nggi yillarda transformer arxitekturalari (BERT va uning optimallashtirilgan varianti DistilBERT) matnlarni semantik mazmuni asosida yuqori aniqlikda tasniflash imkonini berdi. ML.NET va ONNX Runtime kabi texnologiyalar esa oldindan o‘qitilgan modellarni korporativ C#/.NET muhitiga samarali integratsiya qilishga sharoit yaratadi. Mazkur maqolaning maqsadi — konfidensial axborotlarni aniqlash uchun mashinali o‘qitishga asoslangan matn tasniflash modulini ishlab chiqish va uning asosida o‘zbek tilidagi hujjatlar bilan ishlovchi milliy “KARCHKOOT” DLP tizimini yaratib, uning samaradorligini har tomonlama baholashdan iborat.

1.1. Adabiyotlar tahlili. Konfidensial ma’lumotlarning chiqib ketishidan himoyalanish (DLP) yo‘nalishi so‘nggi o‘n yillikda jadal rivojlandi. Liu va Kuhn [1] DLP tizimlarining asosiy tushunchalari va ma’lumot holatlari (data-in-motion, data-in-use, data-at-rest) bo‘yicha nazorat tamoyillarini umumlashtirgan. Shabtai va hammualliflar [2] sizib chiqishni aniqlash va

(cc) BY © O.N.Bozorov

oldini olish yechimlarining keng tasnifini taqdim etgan, Alneyadi va hammualliflar [3] esa mavjud DLP tizimlarini qiyosiy tahlil qilib, ularning aksariyati kontentni chuqur (semantik) tahlil qilish imkoniyatidan mahrum ekanini ko‘rsatgan. Ushbu ishlar muammoning dolzarbligini asoslasa-da, mashinali o‘qitish integratsiyasini cheklangan darajada yoritadi.

Matn kontentini tahlil qilishga asoslangan DLP yo‘nalishida Hart va hammualliflar [4] korporativ hujjatlarni konfidensial va ochiq sinflarga ajratishda matn tasniflash usullarining samaradorligini ko‘rsatgan. Gómez-Hidalgo va hammualliflar [5] esa nomlangan mavjudotlarni aniqlash (NER) orqali shaxsga doir ma’lumotlarning sizib chiqishini bartaraf etish yondashuvini taklif qilgan. Bu ishlar kontentga asoslangan aniqlashning istiqbolini ko‘rsatadi, biroq ular asosan ingliz va boshqa resursga boy tillar uchun mo‘ljallangan.

Matnlarni tasniflashning klassik usullari TF-IDF vaznlash [6] hamda tayanch vektorlar mashinasi (SVM) [7] kabi modellarga tayanadi; Kim [8] esa konvolyutsion neyron tarmoqlarini matn tasniflashga muvaffaqiyatli qo‘llagan. Ushbu usullar samarali bo‘lsa-da, so‘zlarning kontekstual ma’nosini to‘liq hisobga olmaydi. Vaswani va hammualliflarning [9] transformer arxitekturasi va uning asosidagi BERT [10] modeli bu cheklovni bartaraf etib, semantik mazmunga asoslangan tasniflashda yangi bosqichni boshlab berdi. Keyinchalik DistilBERT [11] modeli bilimni distillatsiyalash orqali tezlik va resurs tejashni, RoBERTa [12] va XLM-RoBERTa [13] esa o‘qitish strategiyasi va ko‘p tillilikni takomillashtirdi. Pires va hammualliflar [14] ko‘p tilli BERT modelining tillararo umumlashtirish qobiliyatini tahlil qilgan.

NER yo‘nalishida Lample va hammualliflarning [15] neyron arxitekturalari hamda Yadav va Bethardning [16] sharhi chuqur o‘rganishga asoslangan yondashuvlarning ustunligini ko‘rsatadi. O‘zbek tili kabi kam resursli tillar uchun esa dastlabki ishlar paydo bo‘la boshladi: Mansurovlar [17] o‘zbek tili uchun UzBERT oldindan o‘qitilgan modelini, Salaev v [18] esa SimRelUz semantik baholash to‘plamini taqdim etgan. Shunga qaramay, ushbu ishlar umumiy NLP vazifalariga qaratilgan bo‘lib, axborot xavfsizligi va DLP kontekstiga bevosita moslashtirilmagan.

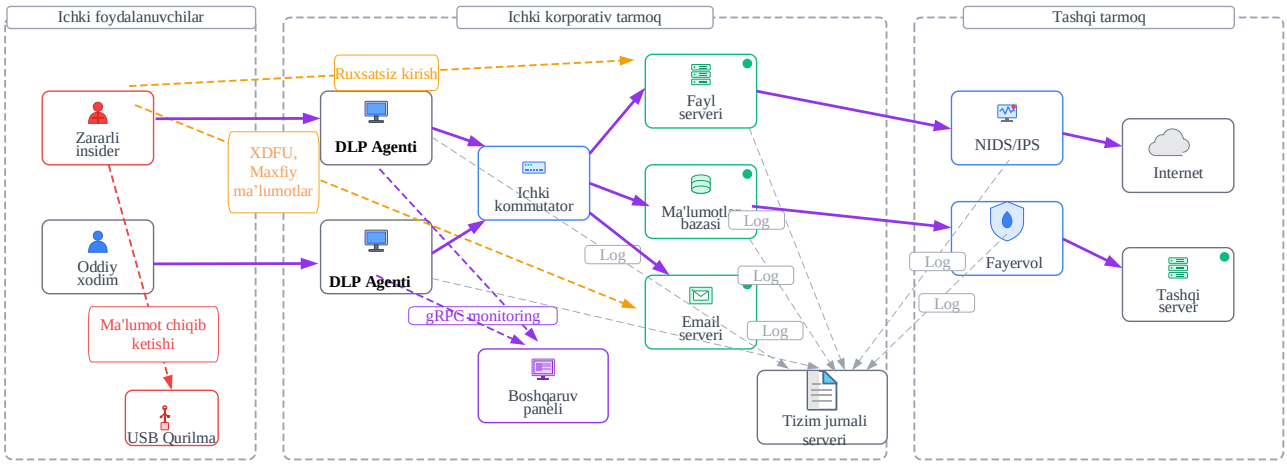
Adabiyotlar tahlili shuni ko‘rsatadiki, bir tomondan DLP arxitekturasi va siyosatiga oid, ikkinchi tomondan matnlarni intellektual tasniflashga oid keng tadqiqotlar mavjud bo‘lsa-da, ushbu ikki yo‘nalishni o‘zbek tili uchun yagona amaliy tizimda birlashtiruvchi yondashuv yetarlicha o‘rganilmagan. Xususan, qoidaga asoslangan, NER va transformer modellarini birlashtiruvchi gibrid tasniflash, uni endpoint darajasida real vaqtli ishlatish hamda model himoyasi masalalari ochiq bo‘lib qolmoqda. Ushbu maqola aynan shu bo‘shliqni to‘ldirishga qaratilgan.

MATERIALLAR VA METODOLOGIYA

2.1. Tizimning umumiy arxitekturasi

“KARCHKOOT” tizimi konfidensial axborotlarni aniqlash, monitoring qilish va boshqarish imkonini beruvchi agent–server arxitekturasiga ega DLP yechimidir (1-rasm). Tizim foydalanuvchi kompyuterlarida ishlovchi DLP-agentlar, markaziy server hamda intellektual tahlil modulidan tashkil topgan. Agent va server o‘rtasidagi muloqot gRPC protokoli orqali tashkil etilib, real vaqtli barqaror ma’lumot almashinuvini ta’minlaydi. Boshqaruv interfeysi Blazor Server platformasida ishlab chiqilgan. Foydalanuvchilarni autentifikatsiyalashda JWT va RBAC, agentlar bilan API muloqotida esa API kalit qo‘llaniladi.

(cc) BY © O.N.Bozorov



1-rasm. "KARCHKOOT" tizimining umumiy arxitekturasi

2.2. Ma'lumotlar to'plami va annotatsiya protokoli

Modelni o'qitish va baholash uchun o'zbek tilidagi 15 000 dan ortiq hujjatdan iborat korpus shakllantirildi. Hujjatlar beshta asosiy sohadan to'plandi: huquqiy (normativ hujjatlar, shartnomalar), moliyaviy (hisobotlar, to'lov ma'lumotlari), kadrlar (xodimlar to'g'risidagi ma'lumotlar), texnik (loyiha hujjatlari) hamda ichki buyruq va xizmat yozishmalari. Har bir hujjat konfidensiallik darajasi bo'yicha belgilandi. Tizim operatsion rejimda uchta darajani (ochiq, konfidensial, maxfiy) ajratsa-da, ushbu maqolada miqdoriy baholash binar masala sifatida olib borildi: «konfidensial» (konfidensial va maxfiy darajalar birlashtirilgan) hamda «ochiq».

Annotatsiya protokoli quyidagicha tashkil etildi. Har bir hujjatni axborot xavfsizligi sohasidagi uch ekspert mustaqil belgiladi; yakuniy belgi ko'pchilik ovozi asosida aniqlandi. Ekspertlararo kelishuv darajasi Koen kappa koeffitsienti bilan o'lchanib, $\kappa \approx 0{,}81$ (yuqori kelishuv) natijasini berdi. Takroriy va deyarli bir xil hujjatlar (dublikatlar) olib tashlandi, maxfiy ma'lumotlar (ism-shariflar, raqamlar) anonimlashtirildi. To'plam tasodifiy ravishda o'qitish, validatsiya va test qismlariga ajratildi (1-jadval).

1-jadval.

Ma'lumotlar to'plamining sinflar bo'yicha taqsimoti

To'plam	O-chiq	Konfi-densial	Jami	Ulush
O'qitish	6 050	4 980	11 030	≈75%
Validatsiya	1 290	1 060	2 350	≈16%
Test	821	500	1 321	≈9%
Jami	8 161	6 540	14 701	100%

2.3. Tasniflash moduli: o'qitish va inferensni ajratish

Tasniflash modulining intellektual yadrosi transformer modeli va ML.NET/ONNX Runtime kutubxonalariga tayanadi. Jarayon ataylab ikki bosqichga ajratildi. O'qitish (training) bosqichi Python muhitida (Hugging Face Transformers, PyTorch) markaziy va himoyalangan serverda bajariladi: bu yerda DistilBERT-base-multilingual-cased modeli o'zbek korpusida fine-tuning qilinadi va ONNX formatiga eksport qilinadi. Inferens (bashorat) bosqichi esa endpointdagi C#/.NET agentida Microsoft.ML.OnnxRuntime orqali amalga oshiriladi. Bunday ajratish o'qituvchi tanlanmani ishchi muhitga chiqarmaslik va modelni endpoint darajasida himoyalash imkonini beradi. ML.NET kutubxonasi qo'shimcha statistik bosqichlar (TF-IDF asosidagi vaznlash, qaror oqimi) uchun ishlatiladi. Modelning asosiy parametrlari 2-jadvalda keltirilgan.

2-jadval.

Tasniflash modelining asosiy texnik parametrlari

Parametr	Qiymat
Arxitektura	DistilBERT-base-multilingual-cased (o'zbek korpusida fine-tuning)
Parametrlar soni	135 million
Transformer qatlamlari	6 (BERT-base — 12)
Yashirin o'lcham / attention heads	768 / 12
Lug'at hajmi (vocabulary)	119 547 token
Maksimal kirish uzunligi	512 token
Model hajmi (ONNX)	540 MB

(cc) BY © O.N.Bozorov

O'qitish: optimizator / validatsiya	AdamW / 20%
O'qitish muhiti / inferens muhiti	Python (Transformers) / C# (ONNX Runtime)
O'rtacha javob vaqti / xotira	≈0,8 – 1,5 s / 700–850 MB

2.4. Gibrid tasniflash va qaror qabul qilishning matematik modeli

Tasniflash aniqligi va qamrovini oshirish maqsadida uchta mustaqil aniqlash mexanizmi birlashtirildi: qoidaga asoslangan aniqlash (kalit so'zlar va regulyar ifodalar), nomlangan mavjudotlarni aniqlash (NER) hamda mashinali o'qitishga asoslangan tasniflash (ML). Gibrid pipeline 2-rasmda keltirilgan. Asosiy qaror qoidasi quyidagi bosqichli funksiya bilan ifodalanadi:

$$D(x) = \begin{cases} C_{rule}(x), & agar\ C_{rule}(x) \neq O; \\ C_{ner}(x), & agar\ C_{rule}(x) = O\ va\ C_{ner}(x) \neq O; \\ C_{ml}(x), & aks\ holda. \end{cases}$$

Bu yerda x — tekshirilayotgan hujjat; $C_{rule}(x)$, $C_{ner}(x)$, $C_{ml}(x)$ — mos ravishda qoida, NER va ML modullarining tasnif natijalari; O — «ochiq» sinf; $D(x)$ — yakuniy qaror. Ushbu ketma-ketlik eng ishonchli va hisoblash jihatidan yengil bosqichdan boshlanadi va bosqichma-bosqich semantik tahlilga o'tadi, shu bilan soxta salbiy (FN) holatlar ehtimolini kamaytiradi.

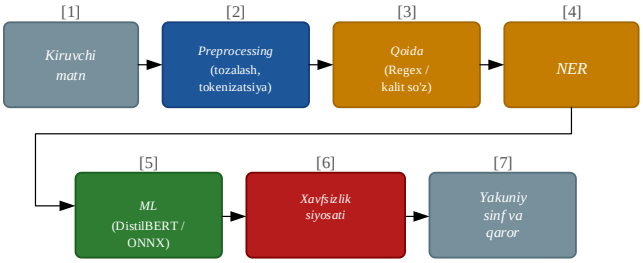
Manbalar ziddiyatli natija bergan murakkab holatlar uchun og'irlikli (weighted) qaror modeli ham qo'llanilishi mumkin. Har bir c sinf uchun umumiy ball quyidagicha hisoblanadi:

$$S_c(x) = w_1 S_{rule,c}(x) + w_2 S_{ner,c}(x) + w_3 S_{ml,c}(x)$$

$$D(x) = \underset{c}{argmax}\, S_c(x)$$

bunda $S_{rule,c}(x)$, $S_{ner,c}(x)$, $S_{ml,c}(x)$— c sinf bo'yicha mos modullarning ishonch ballari; $w1, w2, w3$ — manbalarga berilgan og'irliklar (tajribada $w1 = 0{,}4$; $w2 = 0{,}3$; $w3 = 0{,}3$ qiymatlari qo'llanildi, $w1 + w2 + w3 = 1$). Past ishonchli ($confidence < 0{,}85$) natijalar avtomatik qaror o'rniga qo'lda ko'rib chiqishga yo'naltiriladi.

Statistik o'xshashlik bosqichida matnlar orasidagi yaqinlikni baholash uchun uchta metrika kombinatsiyalandi: Kosinus o'xshashligi uzun, kontekstga boy matnlar uchun yuqori aniqlik (≈0,91), Jakkard o'xshashligi kalit so'zli (policy-based) matnlar uchun eng yaxshi natija (≈0,95), Evklid masofasi esa qisqa yoki kodli iboralar uchun yuqori barqarorlik (≈0,87) beradi. Shu sababli amalda "Jakkard → Kosinus → Evklid" tartibidagi ketma-ket kombinatsiya qo'llanildi; uning hissasi quyida ablation tahlilida baholanadi.



2-rasm. Gibrid tasniflash bosqichlari

2.5. Model faylini himoyalash va tahdid modeli

Sun'iy intellekt modelini mijoz qurilmalarida qo'llashda modelning o'g'irlanishi, teskari muhandislik, modifikatsiya va xotiradan o'qib olish kabi xavflar mavjud. ONNX modelini endpoint darajasida himoyalash uchun ko'p qatlamli yondashuv qo'llanildi: model shifrlangan kanal orqali uzatiladi; mijoz tomonida raqamli imzo va xesh qiymati tekshiriladi; saqlashda Windows Data Protection API (DPAPI) yordamida kalitlar foydalanuvchi va qurilmaga bog'lanadi; inferens jarayonida model ochiq holda diskka yozilmaydi, izolyatsiyalangan muhitda ishlaydi va jarayon tugagach xotira tozalanadi. Tahdidlar va himoya choralari STRIDE yondashuvi asosida 3-jadvalda tizimlashtirilgan.

3-jadval.

Tahdid modeli va himoya mexanizmlari

Tahdid	Tavsif	Himoya mexanizmi
Model theft	ONNX modelni nusxalash/o'g'irlash	Shifrlangan uzatish, DPAPI
Tampering	Model faylini o'zgartirish	Xesh nazorati va raqamli imzo
Replay attack	Eski modelni qayta yuklash	Versiya nazorati
Memory dumping	Xotiradan modelni olish	Izolyatsiya, xotirani tozalash
API abuse	Ruxsatsiz/soxta so'rovlar	API key, JWT, RBAC

2.6. Baholash mezonlari va statistik ishonchlilik

Tasniflash sifati xatoliklar matritsasi (Confusion Matrix) hamda undan kelib chiquvchi mezonlar — Accuracy, Precision, Recall, F1-mezon, soxta ijobiy (FPR) va soxta salbiy (FNR) ulushlari asosida baholandi. DLP tizimlari uchun Recall va FNR ko'rsatkichlari Accuracyga nisbatan muhimroq hisoblanadi, chunki

(cc) BY © O.N.Bozorov

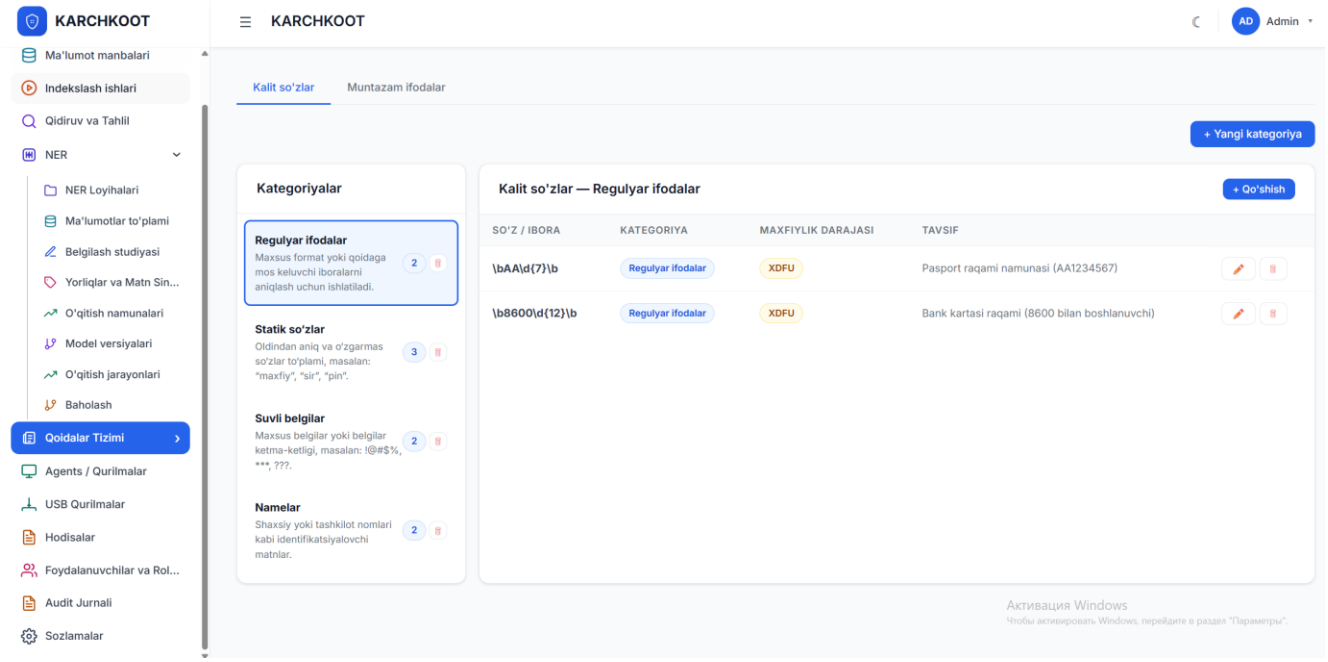
konfidensial hujjatning «ochiq» deb noto‘g‘ri tasniflanishi (FN) bevosita axborot sizib chiqishiga olib keladi. Natijalarning tasodifiy emasligini tasdiqlash uchun 5-karra (k = 5) cross-validation o‘tkazildi, natijalar o‘rtacha ± standart og‘ish ko‘rinishida hamda 95% ishonch oralig‘i (CI) bilan keltiriladi; modellar farqining ahamiyatliligi McNemar testi orqali tekshirildi.

TADQIQOT NATIJALARI

3.1. Tizimning dasturiy interfeysi va monitoring imkoniyatlari

Loyihalashtirilgan korporativ axborot xavfsizligi tizimi oxirgi nuqtalarni nazorat qilish va axborot sizishini bartaraf etishga mo‘ljallangan yaxlit dasturiy majmuadir. Tizim yagona veb-boshqaruv paneli (dashboard) orqali markazlashgan holda boshqariladi. Bosh sahifada aktiv agentlar soni, bugungi hodisalar, ulangan USB qurilmalar va yuqori xavfli insidentlar real vaqt rejimida info-kartochkalar hamda doiraviy diagrammalarda monitoring qilinadi. Tizim tarkibidagi NER (Intellektual matn tasniflash) moduli uzatilayotgan matnlarni real vaqtda semantik klasifikatsiya qiladi; interfeys orqali ma'lumotlar to'plamini belgilash, namunalarni boshqarish, model versiyalarini o'qitish va ularni baholash imkoniyati yaratilgan (3-rasm).

Konfidensial ma’lumotlarni formatlar bo‘yicha avtomatlashtirilgan qidirish uchun tizimda muntazam ifodalar (Regex), statik kalit so‘zlar va maxfiylik darajalarini moslashtirishga mo‘ljallangan qoidalar moduli joriy etilgan (3-rasm). Aniqlangan barcha hodisalar “Hodisalar ro‘yxati” bo‘limida turi, muhimlik darajasi, sana, agent va foydalanuvchi bo‘yicha filtrlash imkoniyati bilan saqlanadi. Tizimning monitoring imkoniyatlari USB faoliyati, fayl hodisalari va haftalik trend diagrammalari kabi grafik ko‘rsatkichlar bilan boyitilgan. Agentlarni boshqarish bo‘limida har bir endpoint kompyuter nomi, IP-manzili, OS va onlayn holati bo‘yicha uzluksiz kuzatiladi. Maxfiy ma’lumot sizishi aniqlangan zahoti, agent foydalanuvchiga real vaqtda ish stoli bildirishnomasini yuboradi va hodisa haqida markaziy panelga signal uzatadi.

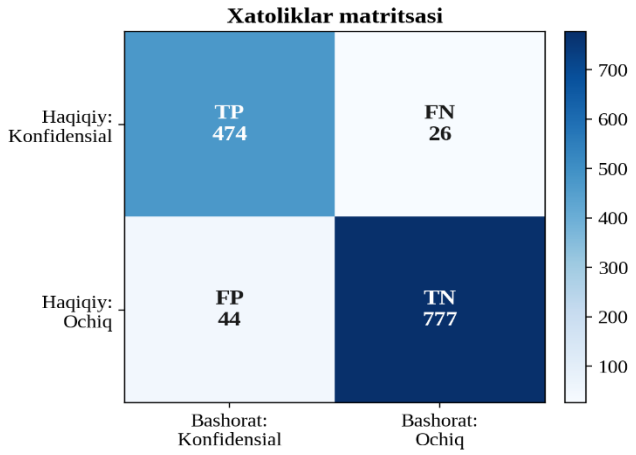


3-rasm. Ishlab chiqilgan DLP tizimining boshqaruv paneli interfeys

3.2. Tasniflash aniqligi va xatoliklar matritsasi

Tizimning tasniflash sifati 1 321 ta test faylida (500 konfidensial, 821 ochiq) binar masala sifatida baholandi. Olingan xatoliklar matritsasi 4-rasmda vizuallashtirilgan: TP = 474, FN = 26, FP = 44, TN = 777.

(cc) BY © O.N.Bozorov



4-rasm. Xatoliklar matritsasi)

Matritsa asosida hisoblangan asosiy mezonlar va ularning 5-karra cross-validation bo'yicha o'rtacha standart og'ish hamda 95% ishonch oralig'i qiymatlari 4-jadvalda keltirilgan. Eng muhimi, soxta salbiy holatlar ulushining past (FNR=5,2%) bo'lishi konfidensial axborotni e'tibordan chetda qoldirish xavfini kamaytiradi.

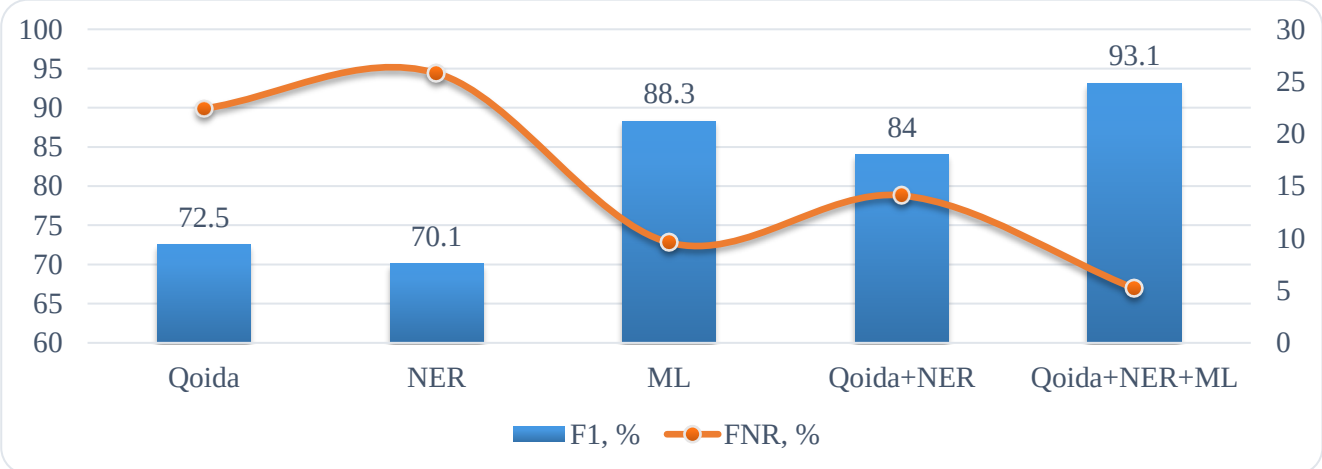
4-jadval.

Tasniflash mezonlari va statistik ishonchlilik

Mezon	Qiymat	O'rtacha	95% CI
Accuracy	94,7%	94,5% ± 0,6%	[93,4%; 95,8%]
Precision	91,5%	91,2% ± 0,9%	[89,8%; 92,9%]
Recall	94,8%	94,6% ± 0,7%	[93,3%; 95,9%]
F1-mezon	93,1%	93,0% ± 0,8%	[91,6%; 94,3%]
FPR	5,36%	5,5% ± 0,6%	[4,4%; 6,7%]
FNR	5,2%	5,4% ± 0,7%	[4,1%; 6,8%]

3.3. Ablation tahlili: gibrid yondashuvning hissasi

Ko'p manbali yondashuvning haqiqiy hissasini baholash uchun ablation tahlili o'tkazildi: har bir modul alohida va kombinatsiyalarda sinovdan o'tkazildi (5-rasm). Natijalar to'liq gibrid (qoida + NER + ML) yondashuv yagona usullarga nisbatan F1 bo'yicha sezilarli ustunlik berishini va FNRni eng past darajaga (5,2%) tushirishini ko'rsatadi. Faqat qoida yoki faqat NER yondashuvlari yuqori FNR bilan ajralib turadi, faqat ML esa yaxshi natija bersa-da, qoida va NER bilan to'ldirilganda eng yuqori umumiy sifatga erishiladi.

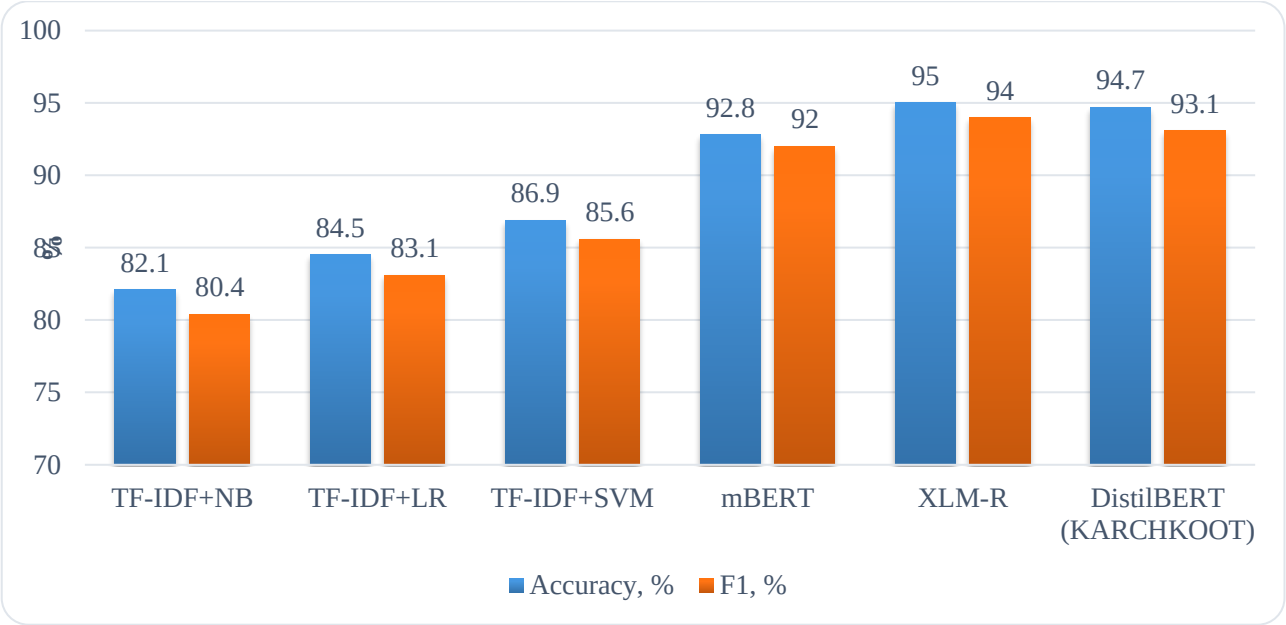


5-rasm. Ablation tahlili: konfiguratsiyalar bo'yicha F1 va FNR

3.4. Baseline modellar bilan qiyosiy tahlil

Tanlangan model asoslanishini ko'rsatish uchun an'anaviy mashinali o'qitish (TF-IDF asosida) va zamonaviy transformer baseline modellari bilan qiyoslash o'tkazildi (6-rasm). DistilBERT asosidagi KARCHKOOT modeli an'anaviy usullardan (TF-IDF + SVM va h.k.) sezilarli ustun bo'lib, mBERT bilan deyarli teng, XLM-RoBERTadan esa biroz past aniqlik ko'rsatadi; biroq DistilBERT inferens tezligi va xotira talabi bo'yicha real vaqtli agent rejimi uchun eng maqbul muvozanatni ta'minlaydi.

(cc) BY © O.N.Bozorov



6-rasm. Baseline modellarning Accuracy va F1 bo'yicha soishtirish

3.5. Model variantlarini tezlik va resurs bo'yicha qiyoslash

Real vaqt tizimi uchun model tanlovini chuqurroq asoslash maqsadida standart BERT-base va DistilBERT taqqoslandi (5-jadval). DistilBERT minimal aniqlik yo'qotishi (−0,5%) evaziga ≈40% tezlik va ≈40% xotira tejashni ta'minlaydi.

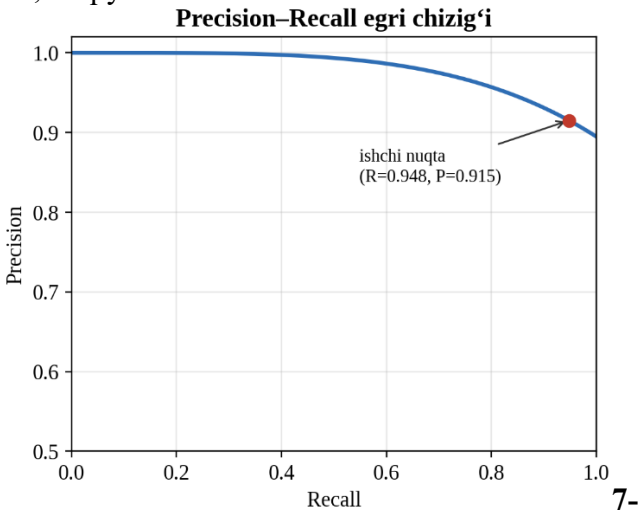
5-jadval.

BERT-base va DistilBERT modellarining tezlik/resurs ko'rsatkichlari

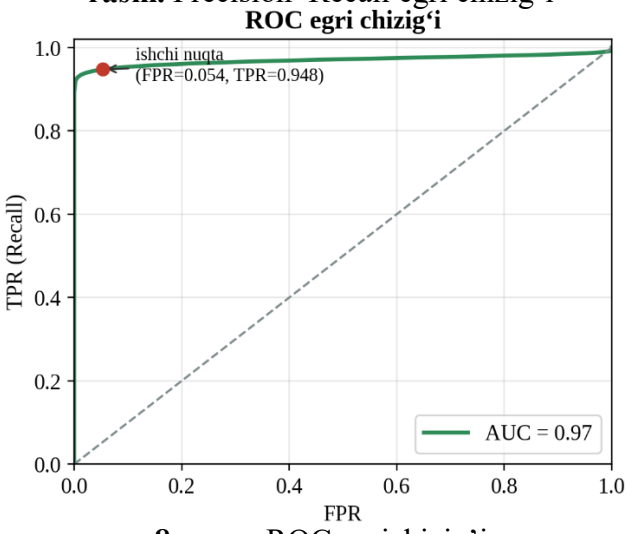
Ko'rsatkich	BERT-base	DistilBERT	Yaxshilanish
Inferens tezligi	1,8–2,5 s	0,8–1,5 s	≈40% tezroq
Xotira	1,2–1,4 GB	0,7–0,85 GB	≈40% kam
CPU yuklamasi	45–55%	25–35%	≈35% kam
Aniqlik	95,2%	94,7%	−0,5%

3.6. Threshold tahlili, ROC va Precision–Recall egrilari

DLP tizimida oddiy Accuracy yetarli emas, chunki eng xavfli holat — konfidensial hujjatni «ochiq» deb o'tkazib yuborish (FN). Shu sababli ishonchlilik chegarasi (threshold) ROC va Precision–Recall egrilari asosida tanlandi (7- va 8-rasm). Chegarani pasaytirish Recallni (va FNRni kamaytirishni) oshiradi, lekin FPRni ko'taradi; chegarani ko'tarish teskari ta'sir beradi. Turli chegaralar bo'yicha FNR va FPR o'zgarishi 6-jadvalda keltirilgan. DLP konteksti uchun FNRni minimallashtiruvchi muvozanatli chegara sifatida ≈0,45 qiymati tanlandi.



7-rasm. Precision–Recall egri chizig'i



8-rasm. ROC egrichizig'i

6-jadval.

Ishonchlilik chegarasiga bog'liq FNR/FPR o'zgarishi

(cc) BY © O.N.Bozorov

Threshold	Recall	Precision	FNR	FPR
0,30	97,8%	86,9%	2,2%	11,4%
0,45	94,8%	91,5%	5,2%	5,4%
0,50	93,4%	92,8%	6,6%	4,3%
0,70	88,1%	95,6%	11,9%	2,1%

3.7. Xatoliklar tahlili (error analysis)

Test natijalaridagi 26 ta soxta salbiy (FN) va 44 ta soxta ijobiy (FP) holat sabablari bo'yicha tahlil qilindi. Asosiy xatolik turlari, ularning sabablari (anonimlashtirilgan misollar asosida) va bartaraf etish yo'llari 7-jadvalda jamlangan. Tahlil shuni ko'rsatadiki, FN holatlar ko'pincha konfidensiallik yashirin/kontekstli ifodalangan yoki lotin-kirill aralash yozilgan matnlarda, FP holatlar esa rasmiy atamalar va ism-shariflar zich uchragan ochiq hujjatlarda yuzaga keladi.

7-jadval.

Xatoliklar tahlili: turlari, sabablari va bartaraf etish yo'llari

Xatolik	Sabab	Misol	Bartaraf etish yo'li
FN	Konfidensiallik yashirin/kontekstli	«loyihaning ichki hujjati»	Semantik modelni kuchaytirish
FN	Lotin-kirill aralash yozuv	«maxfiy / maxfiy»	Normalizatsiya qo'shish
FP	Rasmiy atamalar ko'p	«buyruq», «hisobot»	Thresholdni moslashtirish
FP	Ism-shariflar zich	xodimlar ro'yxati	NER vaznini sozlash

3.8. Obfuskatsiyaga (matnni o'zgartirishga) chidamlilik

Insayderlar konfidensiallikni yashirish uchun matnni ataylab o'zgartirishi mumkin: harflarni ajratish, lotin-kirill aralashtirish, belgilar qo'shish, sinonimlash yoki ochiq matn bilan aralashtirish. Tizimning bunday hujumlarga chidamliligi uchta yondashuv (faqat regex, faqat ML, gibrid) uchun baholandi (8-jadval). Natijalar gibrid yondashuvning obfuskatsiyaga sezilarli darajada chidamliroq ekanini, ayniqsa lotin-kirill aralash va sinonimlash holatlarida regexdan ustunligini ko'rsatadi. Bu yo'nalishda dissertatsiyada ishlab chiqilgan o'zbek tili moslik indeksi algoritmi qo'shimcha himoya beradi (92–96% aniqlik).

8-jadval.

Obfuskatsiyaga bardoshliligini aniqlash darajasi

Obfuskatsiya turi	Faqat regex	Faqat ML	Gibrid yondashuv
Harf almashtirish (m a x f i y)	41%	78%	88%
Lotin-kirill aralash (maxfiy)	23%	81%	90%
Belgilar qo'shish (m@xfiy)	38%	75%	86%
Sinonimlash	19%	83%	89%
Ochiq matn bilan aralashtirish	34%	79%	87%

3.9. Mavjud DLP yechimlari bilan qiyosiy tahlil

"KARCHKOOT" tizimining funksional imkoniyatlari ochiq kodli OpenDLP yechimi bilan qiyoslandi (9-jadval). Taklif etilgan tizim real vaqtli monitoring, kontekstual tahlil, real vaqtli bloklash hamda TF-IDF, NER va ML asosidagi ko'p qatlamli kontent tahlili bo'yicha ustunlikka ega; aniqlik 89% dan 94,7% gacha oshgan, hodisani aniqlash vaqti 120 ms ni tashkil etadi.

9-jadval.

"KARCHKOOT" va OpenDLP tizimlarining qiyosiy tahlili

№	Ko'rsatkich	OpenDLP	KARCHKOOT tizimi
1	Monitoring rejimi	Offline (diskni skanerlash)	Real vaqtli
2	Kontekstual tahlil (vaqt, rol, dastur)	Mavjud emas	Mavjud
3	Real vaqtli bloklash	Mavjud emas	Mavjud
4	Fayl kontentini baholash	Regex, kalit so'zlar	Regex, kalit so'zlar, TF-IDF, NER, ML
5	USB qurilmalarini nazorat	Cheklangan	Qurilma ID va siyosat asosida
6	Kengayuvchanlik	Cheklangan	Moslashuvchan

(cc) BY © O.N.Bozorov

7	Ochiq kodli	Ha	Yo‘q (yopiq prototip)
8	Aniqlik (Accuracy)	89%	94,7%
9	Hodisani aniqlash vaqti	Monitoring oralig‘iga bog‘liq	120 ms
10	Operatsion tizim	Windows, Linux	Windows

4.10. Amaliyotga tatbiq etish va iqtisodiy samaradorlik

“KARCHKOOT” tizimi bir qator davlat tashkilotlarining axborot tizimlarida amaliy sinovdan o‘tkazildi. Sinovlar davomida 12 500 dan ortiq hujjat tekshirilib, to‘g‘ri tasniflash darajasi 92,1% ni tashkil etdi; konfidensial hujjatlarni avtomatik aniqlash jarayoni qo‘lda tahlilga nisbatan 3–4 marta tezlashtirildi, USB orqali sizib chiqish 95% aniqlikda bartaraf etildi (10-jadval).

10-jadval.

Qo‘lda tekshirishga nisbatan samaradorlik

Ko‘rsatkich	**Qo‘lda**	**KARCHKOOT**	**Yaxshilanish**
Hujjat tahlili vaqti	8–12 daqiqa	2–3 daqiqa	3–4 marta tez
Aniqlik	88–91%	92,1–95%	+4–7%
False Negative	7–9%	4,2%	≈−50%
Kunlik qamrov	40–60 hujjat	180–220 hujjat	+300%

Iqtisodiy samaradorlikni baholashda investitsiya qaytimi (ROI) quyidagi formula bo‘yicha hisoblandi:

$$ROI = \frac{B - C}{C} 100\%$$

bunda B — tizim joriy etilgandan keyingi iqtisodiy foyda (tejalgan ish vaqti va kamaytirilgan insidentlar zarari), C — tizimni yaratish va joriy etish xarajati. Hisob-kitoblarga ko‘ra tizim har bir xodim uchun kuniga 4–5 soat vaqtni tejaydi va 8–10 oy ichida o‘zini oqlaydi. Xavfsizlik insidentlarining kamayishi tatbiqdan oldingi va keyingi davrlar bo‘yicha 11-jadvalda keltirilgan.

11-jadval.

Xavfsizlik insidentlarining tatbiqdan oldin va keyin

Davr	**Insidentlar soni (oyiga)**	**Kamayish**
Tizimgacha	≈45	—
Tizimdan keyin	≈15	≈67%

NATIJALAR MUHOKAMASI

Olingan natijalar gibrid tasniflash moduli o‘zbek tilidagi konfidensial hujjatlarni yuqori aniqlikda ajrata olishini ko‘rsatadi. Ablation tahlili ko‘p manbali yondashuvning haqiqiy hissasini tasdiqlaydi: faqat qoida yoki faqat NER yuqori FNR bersa, qoida + NER + ML kombinatsiyasi FNRni 5,2% gacha tushiradi. Baseline qiyoslash shuni ko‘rsatadiki, DistilBERT an’anaviy TF-IDF usullaridan ustun va XLM-RoBERTa kabi og‘irroq modellarga yaqin natija beradi, lekin tezlik/xotira muvozanati bo‘yicha real vaqtli agent uchun afzalroqdir.

DLP nuqtai nazaridan Recall va FNR ko‘rsatkichlari Accuracydan muhimroq, chunki soxta salbiy natija bevosita axborot sizib chiqishiga olib keladi. Threshold tahlili (6-jadval) FNRni minimallashtiruvchi muvozanatli ishchi nuqtani tanlash imkonini berdi. Xatoliklar tahlili (7-jadval) qolgan xatolarning asosan yashirin konfidensiallik va aralash yozuv bilan bog‘liqligini, obfuskatsiya tajribasi (8-jadval) esa gibrid yondashuvning matn o‘zgartirish hujumlariga regexdan ancha chidamliroq ekanini ko‘rsatdi. Tahdid modeli (3-jadval) modelni endpoint darajasida himoyalashning yaxlit asosini beradi.

XULOSA

Ushbu tadqiqotda konfidensial axborotlarni aniqlash uchun mashinali o‘qitishga asoslangan gibrid matn tasniflash moduli ishlab chiqildi va uning asosida o‘zbek tilidagi hujjatlar bilan ishlovchi “KARCHKOOT” DLP tizimi yaratildi. O‘zbek korpusida fine-tuning qilingan DistilBERT modeli ONNX orqali C#/.NET muhitiga integratsiya qilindi; qoida → NER → ML ketma-ketligidagi ko‘p bosqichli qaror qabul qilish mexanizmi va endpoint darajasidagi ko‘p qatlamli model himoyasi taklif etildi.

Binar baholashda tizim 1 321 ta test faylida 94,7% Accuracy, 91,5% Precision, 94,8% Recall va 93,1% F1-mezon ko‘rsatkichlariga erishdi; ablation, baseline, threshold, xatolik va obfuskatsiya tahlillari yondashuvning ilmiy va amaliy asoslanganligini tasdiqladi. Yaratilgan

(cc) BY © O.N.Bozorov

yechim o'zbek tilida ish yurituvchi tashkilotlar uchun milliy DLP infratuzilmasi asosini mustahkamlaydi va kelgusi tadqiqotlar uchun poydevor yaratadi.

FOYDALANILGAN ADABIYoTLAR

1. Liu S., Kuhn R. Data Loss Prevention // IT Professional. 2010. Vol. 12, No 2. P. 10-13.
2. Shabtai A., Elovici Y., Rokach L. A Survey of Data Leakage Detection and Prevention Solutions. Springer, 2012. 92 p.
3. Alneyadi S., Sithirasenan E., Muthukkumarasamy V. A survey on data leakage prevention systems // Journal of Network and Computer Applications. 2016. Vol. 62. P. 137-152.
4. Hart M., Manadhata P., Johnson R. Text Classification for Data Loss Prevention // Privacy Enhancing Technologies Symposium (PETS). 2011. P. 18-37.
5. Gomez-Hidalgo J. M., Martin-Abreu J. M., Nieves J., Santos I., Brezo F., Bringas P. G. Data Leak Prevention through Named Entity Recognition // IEEE Int. Conf. on Social Computing (SocialCom/PASSAT). 2010. P. 1129-1134.
6. Salton G., Buckley C. Term-weighting approaches in automatic text retrieval // Information Processing & Management. 1988. Vol. 24, No 5. P. 513-523.
7. Joachims T. Text Categorization with Support Vector Machines: Learning with Many Relevant Features // Proceedings of ECML. 1998. P. 137-142.
8. Kim Y. Convolutional Neural Networks for Sentence Classification // Proceedings of EMNLP. 2014. P. 1746-1751.
9. Vaswani A. et al. Attention Is All You Need // Advances in Neural Information Processing Systems (NeurIPS). 2017. Vol. 30.
10. Devlin J., Chang M.-W., Lee K., Toutanova K. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding // Proceedings of NAACL-HLT. 2019. P. 4171-4186.
11. Sanh V., Debut L., Chaumond J., Wolf T. DistilBERT, a distilled version of BERT: smaller, faster, cheaper and lighter // arXiv:1910.01108. 2019.
12. Liu Y. et al. RoBERTa: A Robustly Optimized BERT Pretraining Approach // arXiv:1907.11692. 2019.
13. Conneau A. et al. Unsupervised Cross-lingual Representation Learning at Scale (XLM-R) // Proceedings of ACL. 2020. P. 8440-8451.
14. Pires T., Schlinger E., Garrette D. How Multilingual is Multilingual BERT? // Proceedings of ACL. 2019. P. 4996-5001.
15. Lample G., Ballesteros M., Subramanian S., Kawakami K., Dyer C. Neural Architectures for Named Entity Recognition // Proceedings of NAACL-HLT. 2016. P. 260-270.
16. Yadav V., Bethard S. A Survey on Recent Advances in Named Entity Recognition from Deep Learning Models // Proceedings of COLING. 2018. P. 2145-2158.
17. Mansurov B., Mansurov A. UzBERT: pretrained model for the Uzbek language // arXiv:2108.09814. 2021.
18. Salaev U., Kuriyozov E., Gomez-Rodriguez C. SimRelUz: Similarity and Relatedness Scores as a Semantic Evaluation Dataset for Uzbek Language // Proceedings of the 1st Annual Meeting of the ELRA/ISCA SIG on Under-resourced Languages (SIGUL). 2022. P. 56-63.
19. Ahmed Z. et al. Machine Learning at Microsoft with ML.NET // Proceedings of the 25th ACM SIGKDD. 2019. P. 2448-2458.
20. ONNX Runtime: cross-platform, high performance ML inferencing and training accelerator [Elektron resurs]. URL: https://onnxruntime.ai (murojaat sanasi: 10.11.2025).
21. Cohen J. A Coefficient of Agreement for Nominal Scales // Educational and Psychological Measurement. 1960. Vol. 20, No 1. P. 37-46.
22. Dietterich T. G. Approximate Statistical Tests for Comparing Supervised Classification Learning Algorithms // Neural Computation. 1998. Vol. 10, No 7. P. 1895-1923.

(cc) BY © O.N.Bozorov